# UNITED STATES PATENT AND TRADEMARK OFFICE

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/815,191 | 03/31/2004 | Amit Bagga | 503048-US-CIP  (Bagga) | 7508 |

47702          7590          12/24/2008
RYAN, MASON & LEWIS, LLP
1300 POST ROAD
SUITE 205
FAIRFIELD, CT 06824

| EXAMINER |
|---|
| GYORFI, THOMAS A |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2435 | |

| MAIL DATE | DELIVERY MODE |
|---|---|
| 12/24/2008 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on _25 September 2008_.

2a)☐ This action is **FINAL**.       2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) _1-27_ is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-27_ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____ .

## DETAILED ACTION

1.      Claims 1-27 remain for examination.  The correspondence filed 9/25/08 amended

claims 1, 21, and 27.

### *Continued Examination Under 37 CFR 1.114*

2.      A request for continued examination under 37 CFR 1.114, including the fee set

forth in 37 CFR 1.17(e), was filed in this application after final rejection.  Since this

application is eligible for continued examination under 37 CFR 1.114, and the fee set

forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action

has been withdrawn pursuant to 37 CFR 1.114.  Applicant's submission filed on 9/25/08

has been entered.

### *Response to Arguments*

3.      Applicant's arguments, see the amendment filed 9/25/08 with respect to the

rejection(s) of claim(s) 1-27 under P-Synch in view of SecurityStats have been fully

considered and are persuasive.  Therefore, the rejection has been withdrawn.

However, upon further consideration, a new ground(s) of rejection is made in view of the

newly discovered OneLook Dictionaries reference(s).

### *Claim Rejections - 35 USC § 103*

4.      The text of those sections of Title 35, U.S. Code not included in this action can

be found in a prior Office action.

5.      Claims 1-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over the

P-synch version 6.2 software product, as evidenced by the "P-Synch Installation and

Configuration Guide" (hereinafter, "P-Synch"), in view of the web page

"SecurityStats.com Password Strength Meter" (hereinafter, "SecurityStats.com") in view

of the "OneLook Dictionary" search engine (collectively hereinafter, "OneLook").[1]


Regarding claims 1, 21, and 27:

        P-Synch discloses a method, apparatus, and article of manufacture for

evaluating a password proposed by a user during an enrollment process (page 21, "5.3

Accounts on target systems") comprising: receiving said proposed password from said

user (page 4, "3. Users select a new password..."); evaluating results from a table

lookup relative to one or more predefined thresholds (page 4, "4. P-Synch checks the

new password..."; cf. pages 124-126, but particularly those rules on page 126 as

indicated); and rejecting said proposed password when said user is correlated with said

proposed password if one ore more of said predefined thresholds are exceeded by said

results (Ibid).  With respect to claim 21, P-synch is installed on a server (page 28, "1.

Prepare a P-Synch server..."), which inherently possesses memory and a processor

coupled to said memory.

        P-Synch does not explicitly disclose performing an Internet search using a query

containing one or more keywords derived from said proposed password.  However, it is

---

[1] Although page 1 of OneLook is a separate web page from the remaining 37 pages, each web page
incorporates the other by reference ("Browse Dictionaries" links on page 1; "Home" link on pages 2 & 38,
respectively) and thus for purposes of examination have been considered as a single prior art reference.

observed that P-synch, while already possessing a defined set of rules to measure a

proposed password's strength, can nevertheless be extended by allowing an admin to

add new rules via a plugin (page 127, section 10.19.1 "Adding new rules with a plugin

program"). Furthermore, it is observed that P-Synch is essentially a web application, in

that users interact with P-Synch via a web browser (page 6, "2.2.1 User Interfaces"; cf

Figure 10.3 on page 93) and P-Synch is capable of interacting with other web sites via a

web interface (see the "HTTP apps" and "HTTPS apps" on page 20; cf. the sample

scripts for interacting with a website on pages 327 & 328). Moreover,SecurityStats.com

discloses a publicly available web site on the Internet that one may query to determine if

a password is sufficiently strong (see page 1). Additionally, SecurityStats.com

recommends not using the actual proposed password but rather something similar [i.e.

a keyword] to perform the query (page 1, 2$^{nd}$ paragraph). Thus the claim is obvious

because all the claimed elements were known in the art, and one of ordinary skill in the

art could have combined the elements as claimed by known methods (i.e. writing a

plug-in for P-Synch to use P-Synch's web interface to query SecurityStats.com as a

new password strength rule), and the combination would have yielded predictable

results to one of ordinary skill in the art at the time of the invention.

It is noted that SecurityStats.com discloses checking a single dictionary to

evaluate a proposed password's strength (page 1, first paragraph), although it suggests

that one should avoid using a password that appears in any of a plurality of dictionaries

and the like (the first "DO NOT" on page 2). Although the technical details of how

SecurityStats.com checks a dictionary is not disclosed in that reference, OneLook

discloses wherein it had been known well before the time of the instant invention that

one could use a search engine (OneLook: page 1) to search a plurality of web sites (at

that time, 745 online dictionaries and word list sites: pages 2-38) to find a particular

term.  It would have been obvious to modify SecurityStats.com (particularly as would be

applied to P-Synch above) to search a plurality of [dictionary] web sites using a search

engine in order to determine if a proposed query is indicative of a weak password, as

opposed to checking the single dictionary as was originally disclosed, as OneLook

establishes that this technique was clearly within the capabilities of one of ordinary skill

in the art.  Examiner also observes that the general technique of duplicating a part for a

multiple effect (e.g. searching many dictionaries instead of one) has been held by the

courts to be obvious: see *In re Harza*, 274 F.2d 669, 124 USPQ 378 (CCPA 1960).


Regarding claims 2, 3, and 22:

    P-Synch further discloses wherein said one or more predefined correlation rules

evaluate whether that said proposed password can be [qualitatively: the password is the

username; quantitatively: the password is similar to the username] correlated with said

user (page 126, as indicated).


Regarding claims 4, 6, 23, and 24:

    P-Synch further discloses wherein said proposed password is comprised of a

proposed answer and a proposed hint (the user Q&A profiles on pages 83 and 199-200.

Although P-Synch has many rules by which one can correlate a proposed password to

known weak passwords, P-Synch does not explicitly disclose determining whether the

proposed answer can be correlated to/obtained from the proposed hint (i.e. the

proposed password should not be similar to any of the personal information used in

establishing one's personal profile – see also page 6, "2.2.2 Authentication System").

However, P-Synch discloses that one can augment the rules by which it determines the

strength of proposed passwords (via external plug-ins, page 126; cf. sections 10.19.1

and 10.19.2 on pages 127-128) developed using techniques that one of ordinary skill in

the art would have known (pages 576-584), said plug-ins allowing P-Synch to query

additional sources for password strength rules (Ibid).  Furthermore, SecurityStats.com

teaches that it was common knowledge among those of ordinary skill in the art that the

various kinds of information already retained by P-Synch for a user's personal profile

(the hints and answers), makes for very weak passwords (the "DONT'S" list on pages 1-

3).  It would have been obvious to one of ordinary skill in the art at the time the invention

was made to develop a plug-in for P-Synch, in accordance with the techniques explicitly

disclosed for that exact purpose, that would have allowed it to query the user's personal

profile to see if the proposed answer correlates to [i.e. is an anagram of], or can be

obtained from [i.e. is an exact match for], the password hint.  All the claimed elements

were known in the prior art and one skilled in the art could have combined the elements

as claimed by the disclosed methods, and the combination would have yielded

predictable results to one of ordinary skill in the art at the time of the instant invention.

Regarding claim 5:

P-Synch further discloses wherein said particular relation is selected from the

group consisting essentially of self, family member, co-author, teammate, colleague,

neighbor, community member, or household member (pages 83, 199, & 200).


Regarding claims 7 and 25:

P-Synch further discloses wherein said proposed password is an identifying

number (e.g. PIN number, e.g. page 6, "2.2.2 Authentication Systems").


Regarding claims 8, 10, 11 and 26:

Although P-Synch discloses wherein said proposed password is an identifying

number, it does not explicitly disclose rules to determine if the identifying number meets

any of the following criteria: whether said identifying number identfies a person in a

particular relationship to said user [claims 8 and 26], identifies a top N commercial entity

[claim 10], or identifies said user [claim 11]. However, P-Synch maintains a database

with each of those pieces of information: a number that identifies a person in a particular

relationship to said user ("Family member phone number that is not your own", pages

83 and 200), a top $N^2$ commercial entity (radio station dial number, Ibid), and the user

("Your SSN", Ibid). P-Synch further discloses that one can augment the rules by which

it determines the strength of proposed passwords (via external plug-ins, page 126; cf.

sections 10.19.1 and 10.19.2 on pages 127-128) developed using techniques that one

---

[2] For purposes of the rejection of claim 10, it is assumed that N=1.

of ordinary skill in the art would have known (pages 576-584), said plug-ins allowing P-Synch to query additional sources for password strength rules (Ibid). Furthermore, SecurityStats.com teaches that it was common knowledge that each piece of personal information known to be recorded by P-Synch makes for a very weak password (the "DONT'S" list on pages 1-3). It would have been obvious to one of ordinary skill in the art at the time the invention was made to develop a plug-in for P-Synch, in accordance with the techniques explicitly disclosed for that exact purpose, that would have allowed it to query the user's personal profile to evaluate whether the identifying number meets any of the recited criteria in these claims. All the claimed elements were known in the prior art and one skilled in the art could have combined the elements as claimed by the known methods, and the combination would have yielded predictable results to one of ordinary skill in the art at the time of the instant invention.

Regarding claim 9:

P-Synch further discloses wherein said one or more pre-defined correlation rules evaluate whether said identifying number is a top N most commonly used identifying number (in the embodiment where the password is a PIN, the password history rules on pages 126 and 127).

Regarding claims 12-14:

P-Synch further discloses wherein said identifying number is a portion of a telephone number, address, or social security number (pages 83 and 200).

Regarding claim 15:

      P-Synch further discloses wherein said proposed password is a word (page 125, the dictionary rules).

Regarding claim 16:

      P-Synch further discloses wherein said one or more predefined correlation rules evaluate whether a correlation between said word and said user exceeds a predefined threshold (e.g. the last two rules on page 125).

Regarding claim 17:

      P-Synch further discloses wherein said correlation is determined by performing a meta-search (searching in accordance with rules found in one or more external plug-ins and/or the password history table, page 126).

Regarding claim 18:

      P-Synch further discloses wherein said step of ensuring a correlation further comprises the step of performing a meta-search (Ibid).

Regarding claim 19:

      P-Synch further discloses wherein said step of ensuring a correlation further comprises the step of performing a local proximity evaluation (e.g. the last two rules on page 125, and the variants of the username on page 126).

Regarding claim 20:

P-Synch further discloses wherein said step of ensuring a correlation further

comprises the step of performing a number classification (the digits rules: page 125).


## *Conclusion*

6.     Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Thomas Gyorfi whose telephone number is (571)272-

3849.  The examiner can normally be reached on 8:30am - 5:00pm Monday - Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's
supervisor, Kim Vu can be reached on (571) 272-3859.  The fax phone number for the
organization where this application or proceeding is assigned is 571-273-8300.
Information regarding the status of an application may be obtained from the
Patent Application Information Retrieval (PAIR) system.  Status information for
published applications may be obtained from either Private PAIR or Public PAIR.
Status information for unpublished applications is available through Private PAIR only.
For more information about the PAIR system, see http://pair-direct.uspto.gov. Should
you have questions on access to the Private PAIR system, contact the Electronic
Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a
USPTO Customer Service Representative or access to the automated information
system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.


TAG
12/10/08
/Kimyen  Vu/
Supervisory Patent Examiner, Art Unit 2435